Changing DoD's IT Capabilities

Delivering and Defending the Network

Lt. Gen. Charles E. Croom, USAF
Director, Defense Information Systems Agency and
Commander, Joint Task Force for Global Network Operations

Hackers attempt to break into a Department of Defense network and are blocked. A military doctor pulls up an online medical record for an injured servicemember. A remotely deployed servicemember uses a satellite system to relay information. The Defense Information Systems Agency and the Joint Task Force for Global Network Operations are involved in all those scenarios. Air Force Lt. Gen. Charles E. Croom, DISA director and JTF-GNO commander, talked to *Defense AT&L* in January 2008 about what's next for those organizations, especially as technology continues to change.

Q.
You've served as the director of the Defense Information Systems Agency and the commander of the Joint Task Force for Global Network Operations since July 2005. Can you give us an overview of your roles and responsibilities?

A.
As you mentioned, I wear two hats as both the director of DISA and commander of the JTF-GNO. DISA is the materiel provider of joint IT solutions for the Department of Defense. The JTF-GNO team, under U.S. Strategic Command, is responsible for operating and defending the network. Although DISA and the JTF-GNO have different responsibilities, they are engaged in complementary efforts driving improvements to how our current network is designed, implemented, operated, and defended during this time of dynamic information technology changes. At the same time, both organizations are trailblazing solutions that

> "Delivering IT is a team sport."

Photos by Donna Burton, DISA

allow U.S. military members to more freely exchange information wherever they are in the world while, at the same time, protecting that information.

Q.

You have said previously that to capture today's technology for DoD, DISA has recognized a need to change the way it does business, particularly in regards to improving the time needed to get services and technology into the hands of the warfighter. Can you describe the ways that DISA is working to speed up the processes of acquisition and testing?

A.

Successful delivery of IT capabilities to the warfighter, our primary customer, requires a team effort. DISA has been working closely with our growing number of government and industry partners to more rapidly acquire and test IT services. We're working together using both legacy and new processes that allow us to make capabilities available faster. Central to this has been the "Adopt, Buy, Create" approach we've used across the agency. With the ABC approach, we first seek to leverage the forward-leaning work of other government organizations. We adopt promising solutions and make them available across the network. One example is adopting the 2-million-user Army Knowledge Online as DoD's portal, Defense Knowledge Online. Also, we've been successful in buying powerful industry solutions for the department, such as the enterprise collaboration services, which we call "Button 1" and "Button 2." Both of these collaboration tools are now available via the DKO portal.

Effective testing is essential to successful implementation of enterprise solutions. Approaches such as early user testing are allowing us to make services available faster and gain the information we need to support risk-based decisions about the next implementation steps to take and to scale the service appropriately. Testing processes are becoming increasingly collaborative. For example, the Federated Development and Certification Environment will leverage technology to bring the developers, warfighters, testers, and certifiers together as early in the process as practical to do more simultaneously, instead of sequentially, to reduce the time it takes to get needed capabilities to the field.

Q.

What about the challenge of changing people's mindsets towards how they do business? Many Service applications have been purchased with a specific need in mind, and many people are accustomed to working with applications and information-sharing devices in ways that they've done in the past. What is DISA doing to change that mindset?

A.

I used to think along the lines of the old saying, "If it ain't broke, don't fix it." Looking at our world today, the reality is that if you're not changing, not looking for ways to provide improved services and/or capabilities, you're falling behind. At the same time, we have many legacy systems in the DoD that are currently filling a need for a limited community but aren't yet broadly available to support the joint warfighter.

We're making exciting headway toward establishing the service-oriented architecture foundation and gaining consensus on shared standards and specifications, which will allow Web services to be available across the enterprise. Some teams have already moved out with pilot efforts that exercise these new capabilities, like Maritime Domain Awareness. The MDA effort has been successful in allowing the community to share knowledge of the global maritime environment through exploitation and visualization of legacy and emerging data sources from the Navy, Coast Guard, and Department of Transportation. Programs like the Net-Enabled Command Capabilities and the Global Electromagnetic Spectrum Information System will also take advantage of these core services and standards to allow services and data to be more readily shared between those who have the information and those who need it.

Q.

DISA's statistics have stated that DoD is roughly doubling its data traffic every two years. How is your agency responding to this need for increased bandwidth, and what is your agency's long-term plan for providing bandwidth to the warfighter in the future?

A.

Over the years, DISA has been actively alert to network traffic growth and uses a variety of tools to measure and track bandwidth utilization on the NIPRNet [*Unclassified but Sensitive Internet Protocol Router Network*] and SIPRNet [*Secret Internet Protocol Router Network*]. Increases in use of the Defense Information System Network core and Internet access have been significant factors related to bandwidth growth. Our NIPRNet and SIPRNet traffic stats indicate that data traffic is approximately doubling every two years. The good news is that, so far, we've been able to stay ahead of the need.

Besides making information available more rapidly across the DoD, net-centric enterprise applications are also impacting network usage. Network managers are providing close monitoring to allow them to continuously rightsize the networks, thus ensuring high performance. As more warfighter requirements move to Internet protocol, DISA will continue to ensure that the NIPRNet and SIPRNet are sufficiently sized to meet those needs.

Realistically, not every location will be connected by cable or be rich in bandwidth. For these situations, we'll need to look to other options. Enterprise collaboration service

Lt. Gen. Charles E. Croom, USAF

Director, Defense Information Systems Agency and Commander, Joint Task Force for Global Network Operations

Lt. Gen. Charles E. Croom is the director of the Defense Information Systems Agency and the commander of the Joint Task Force for Global Network Operations. As DISA director, he leads a worldwide organization of more than 6,600 military and civilian personnel. This organization plans, develops, and provides interoperable command, control, communications, computers, and information systems to serve the needs of the president, secretary of defense, Joint Chiefs of Staff, combatant commanders, and other Department of Defense components under all conditions during peace and war. As the JTF-GNO commander, Croom is responsible for directing the operation and defense of the Global Information Grid to assure timely and secure net-centric capabilities across strategic, operational and tactical boundaries in support of DoD's full spectrum of warfighting, intelligence, and business missions.

Croom entered the Air Force in 1973 as a distinguished graduate of the Rutgers University ROTC program, where he was the commandant of cadets. His past assignments include serving as the director of communications, Headquarters, Air Mobility Command; director of mission systems, deputy chief of staff for communications and information, Headquarters, U.S. Air Force; director of command, control, and communications systems, Headquarters, U.S. European Command; vice director for command, control, communications, and computer systems, the Joint Staff; and director of command, control, communications, computers, intelligence, surveillance, and reconnaissance infostructure, deputy chief of staff for warfighting integration. Prior to his current assignment, Croom was the director of information, services, and integration, Secretary of the Air Force Office of Warfighting Integration.

Croom has received the Defense Superior Service Medal with oak leaf cluster, the Legion of Merit, the Defense Meritorious Service Medal with oak leaf cluster, the Meritorious Service Medal with three oak leaf clusters, the Joint Service Commendation Medal, and the Air Force Commendation Medal. He will retire in July 2008.

Button 2, currently in early user testing, supports XMPP [*Extensible Messaging and Presence Protocol*]-enabled low bandwidth chat, a capability well-suited for environments where bandwidth is limited. Also in the pipe are pilot efforts such as Tactical Service Provider. TSP is a joint capability technology demonstration working with the Army, U.S. Central Command, U.S. Transportation Command, and U.S. Joint Forces Command that is exploring a hybrid next-generation satellite and wireless communications architecture that will more effectively extend the DISN core network services out to the remote and mobile warfighter.

The electromagnetic spectrum is currently a hot topic. In Iraq, we've learned that improvised explosive devices can be detonated remotely using wireless technologies. It's also a hot topic in industry, which needs spectrum for consumer products such as cell phones and Blackberry® devices.

Q.

Speaking of spectrum, the Defense Spectrum Organization falls within DISA's responsibilities. Can you describe how the DSO has been working to support the warfighter, and how the DSO is working to protect spectrum that the military needs?

A.

The DSO was established in the summer of 2006, combining the Defense Spectrum Office and the Joint Spectrum Center into one organization that would better address the many challenges of our spectrum environment. For example, when the Joint Staff released a Joint Urgent Operational Needs Statement citing the need for better spectrum support in theater, the JSC stood up a 24/7 Spectrum Analysis Cell and also sent personnel forward to train, assist, and troubleshoot electromagnetic interference in Iraq and Afghanistan. The positive news is that after 16 months, the forward team has been very effective in its troubleshooting and training efforts and is being released to return home. The JSC, of course, will continue to support any spectrum challenges that arise in theater.

As a leader in the department's efforts to transform spectrum operations, DSO is also central to developments that will allow DoD to effectively and efficiently use spectrum, especially as competition for spectrum increases around the world. Several efforts are under way to leverage technologies to ease the impact of the competition. One of these efforts, dynamic spectrum access, affords the opportunity to better utilize the spectrum, allowing more users on a given frequency at a given location than the current reservation process allows. Dynamic spectrum access can also reduce interference because spectrum-dependent systems may sense the environment and transmit for very brief periods of time. As dynamic-spectrum-access technology, policies, and procedures mature, they may

provide the opportunity to realize bandwidth on demand worldwide.

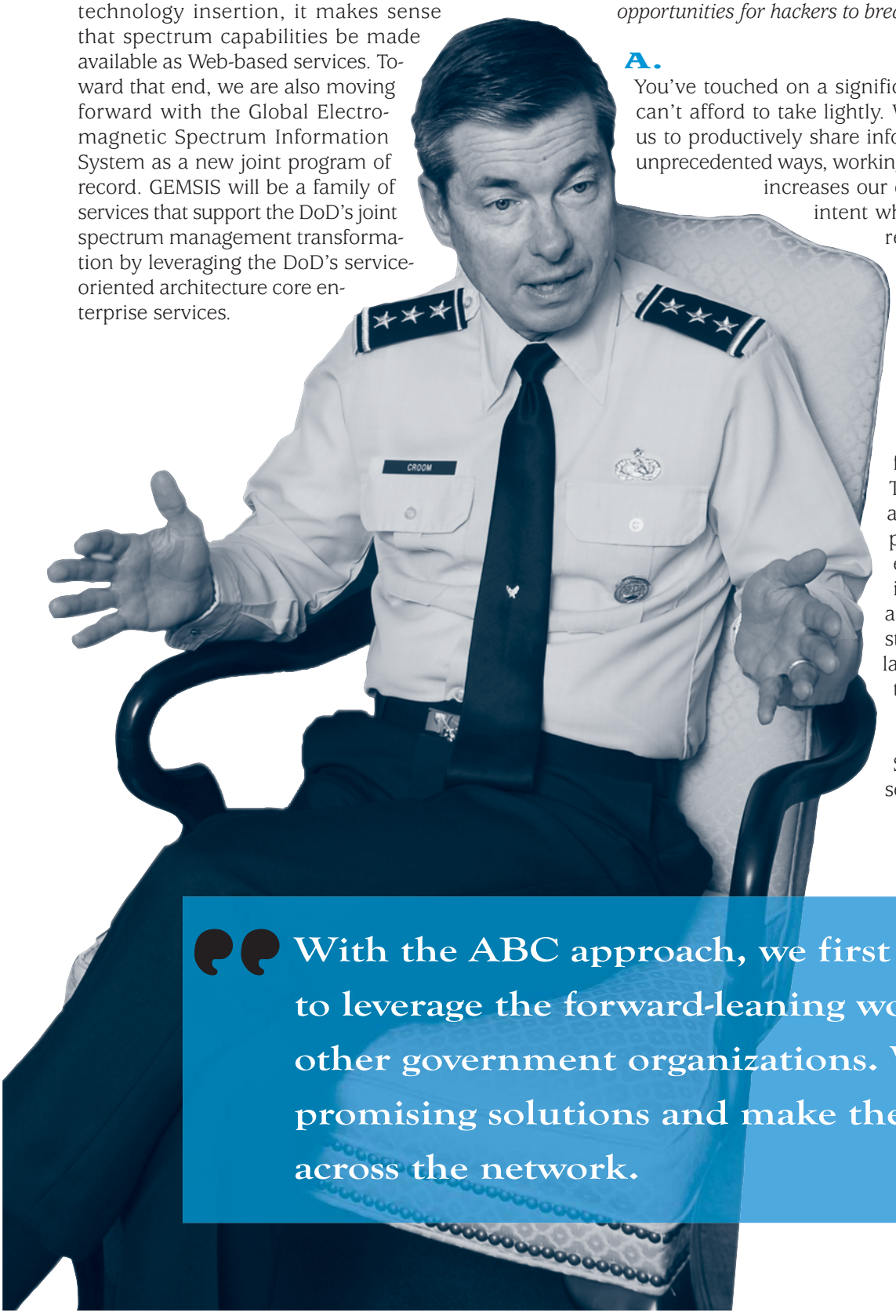
Since transforming spectrum management is as much about business process improvements as it is about technology insertion, it makes sense that spectrum capabilities be made available as Web-based services. Toward that end, we are also moving forward with the Global Electromagnetic Spectrum Information System as a new joint program of record. GEMSIS will be a family of services that support the DoD's joint spectrum management transformation by leveraging the DoD's service-oriented architecture core enterprise services.

Q.

Many computer applications were previously designed to run on closed networks, but an increasing number are now being run using the World Wide Web. While this allows for greater information sharing, doesn't it also mean greater opportunities for hackers to break into DoD systems?

A.

You've touched on a significant set of challenges we can't afford to take lightly. While the Internet allows us to productively share information in powerful and unprecedented ways, working in that environment also increases our exposure to those with ill intent who operate there. With its responsibility to operate and defend the Global Information Grid, currently made up of about 7 million computers and 15 thousand networks worldwide, the Joint Task Force for Global Network Operations utilizes a "defense in depth" approach. The approach includes a combination of strong perimeter defense; client-based security; user identity management; and partnering with other stakeholders, which include law enforcement organizations such as the National Security Agency and the Department of Homeland Security. Of course, an essential ingredient to success



> **With the ABC approach, we first seek to leverage the forward-leaning work of other government organizations. We adopt promising solutions and make them available across the network.**

is active participation from those who use the network, including all of the DoD military services and agencies.

We're seeing positive trends with the efforts to date, such as a decrease in root-level intrusions. However, those who want access to the networks and the department's information are persistently trying new ways to achieve their aims. To counter the threat, efforts are under way toward more machine-to-machine automated and aggregated reporting to achieve the situational awareness our various network health and security sources can provide. Already piloted at 23 sites, the host-based security system is in the process of being implemented across the Global Information Grid. HBSS, the largest fielding of an information assurance tool in DoD history, allows awareness and security to the desktop. We're also moving forward with the second phase of common access card/public key infrastructure implementation. So far, about 93 percent of DoD is using CAC/PKI to access the network. We've learned that business processes and application requirements are currently the primary reasons for users not employing CAC for network log-in. Our next actions will involve improving access to the NIPRNet with CAC/PKI or secure alternate token and providing additional metrics and granularity to facilitate development of technical solutions that will allow CAC usage to reach 100 percent.

Q.

Developing interoperable communications solutions for U.S. allies is a challenge because of different equipment, software programs, and even different outlets. Yet the United States has had up to 26 allies helping to support its operations in Iraq—there needs to be communication between all. What is DISA doing to address the need for communications between its coalition partners?

A.

This is another area where we are placing increased emphasis. Information sharing with our mission partners beyond the U.S. joint arena is currently accomplished through numerous stove-piped network domains, including different versions of the Combined Enterprise Regional Information Exchange System. As a result, today's operators must often "swivel chair" between coalition and national systems to have full battlespace awareness, and data must be entered multiple times between the separate systems.

> "We're shifting our mindset from work being 'a place to go' toward work being 'something you do.'"

In March 2007, the Net-Centric Functional Capabilities Board endorsed a set of requirements for the CENTRIXS Cross-Enclave Requirement to converge multiple CENTRIXS enclaves to a single infrastructure. This fiscal year will see the establishment of a test and integration lab and actions that will promote a more seamless interchange of multinational data, including a more effective disclosure policy. Advancements toward this end will be tested dur-

ing the Coalition Warrior Interoperability Demonstration 2008. The team making this all happen, which includes several combatant commands, will take the lessons we gain from CWID and other demonstrations forward to meet the Net-Centric Functional Capabilities Board's requirements supporting multinational missions.

Q.

Open-source software has the potential to save DoD a considerable sum. DISA's leadership has spoken about considering such software. Can you describe the challenges of allowing open-source software into DoD, and what is being done to address those challenges?

A.

The Department of Defense is already using open source software in countless critical applications like the Berkeley Internet Name Domain software that provides name resolution on DoD networks and the global Internet. Red Hat Linux® operating systems are used to host the DoD's PKI servers, and Apache® Web software is used to serve countless DoD Web pages.

We are now seeking to expand the role of open-source software in the department to be able to maximize the value of open-source software and development methodologies while minimizing its risks to the department. First, we have established an Open Source Steering Group, which brings together open source developers from DISA, across DoD, academia, and industry to develop and evaluate open source development methodologies, identify and review existing open-source efforts that can benefit DoD, provide consulting to developers and acquisition professionals on the use of open source, and bring together a community of open source developers to solve DISA and DoD problems. Some of the early successes of the OSSG are DoDBastille, which automates the lockdown of Linux operating systems to DoD security standards; DoDSST, which provides similar functionality for Solaris; and LinuxCAC, which supports the DoD's CAC for open source operating systems. These early success projects are in use in either the lab environment or in operational systems.

Second, DISA is looking to enable collaborative, open source software development as a component of our Federated Development and Certification Environment. We believe this will reduce the costs of open- and shared-source software development, encourage software re-use, and reduce time to market by adopting approaches and tools already in use by the open-source community.

Q.

In August 2003, DISA created the full-time position of the component acquisition executive and, shortly after, DISA developed a program executive officer-like capability under the CAE. How has this structure benefited DISA?

A.

As you mentioned, the CAE is now appropriately a full-time position, not a collateral duty. Diann McCoy performed superbly in this role until her recent retirement in January 2008. She charted a solid course on the unpaved trail toward net-centricity, leveraging her extensive experience and lessons learned from the acquisition rulebook. Although we will miss Diann's leadership, I'm pleased that another outstanding acquisition leader will be filling her shoes: Tony Montemarano. Tony's prior results, like his successful delivery of the GIG-Bandwidth Expansion Program, bode well for the agency as he assumes the role of CAE.

DISA's move to a PEO structure was not taken lightly. Before standing up the current PEO structure, we conducted a comprehensive review of 89 programs and projects, looking at appropriate authorities and alignment to better deliver joint IT capabilities. The resulting current structure encompasses PEOs for command and control capabilities; global information grid enterprise services; information assurance/NetOps; and satellite communications, teleport, and services. All are led by some of our most effective senior executive service leaders in the agency, who report to the CAE. I believe the structure provides an appropriate level of insight to our PEO directors to ensure the appropriate level of interaction between the programs and projects within their portfolio. This, along with quarterly program reviews, has given the DISA team an unprecedented level of awareness to leverage the dependencies between the programs.

Another important element of this model is the CAE's responsibility for maintaining a professional acquisition workforce in spite of the widely reported shortfall in the career field. As a leader in DoD joint acquisition, DISA must maintain a skilled, professional acquisition workforce. Internal and external training, career broadening and advancement opportunities, quality of life benefits, and the fact that each program's DAWIA [*Defense Acquisition Workforce Improvement Act*] certifications status is reviewed at quarterly IPRs [*in process review*], all contribute to DISA maintaining a strong acquisition team.

Q.

Your agency's telework program is one of the strongest in the federal government. Can you talk more about the benefits and challenges of DISA's teleworking initiatives?

A.

We believe that, when done correctly, employees who telework are just as, or even more, happy and productive than when they are in the traditional office. We're shifting our mindset from work being "a place to go" toward work being "something you do." For those interested in teleworking, DISA provides a laptop computer loaded with virtual private network software and pays for 50 percent

> Much as a homeowner pays for utilities, these capacity service contracts allow us to pay for only the CPU-hours or gigabytes of storage we use in our computing centers.

of the monthly broadband expense into the employee's home. Employees just need a high-speed Internet connection, either at their residence or a telework center, and their supervisor's approval.

We are also always looking for ways to improve the telework program. We hold training classes for managers and brown bag sessions at several locations, and the feedback received during these gatherings is already being used to make changes.

I've also just approved a change to our policy which allows employees to telework three days per week with their supervisor's approval. We are also continuing to emphasize the requirement for a work plan for each teleworking employee and a continued focus on measuring productivity. If you can demonstrate there is an increase in productivity, who can argue with that? Also of note is that DISA's telework policy is not limited to DISA's headquarters or to the National Capital Region, and we're pleased to see that more and more folks across the agency are taking advantage of this opportunity. I expect that telework will continue to be an important component of DISA's recruitment and retention strategy.

Q.

You've mentioned previously that DISA's annual budget comes mostly from your customers, and that one of DISA's strategic goals is providing "best value" for your customers. How is DISA progressing toward that goal?

A.

About 75 percent of DISA's annual budget comes from our customers, and we are making significant progress toward providing them best value and improved financial transparency. About a year ago, we awarded capacity-on-demand computing contracts for both processing and storage services. These contracts have given us some attractive opportunities for flexibility and cost savings. Much as a homeowner pays for utilities, these capacity service contracts allow us to pay for only the CPU-hours or gigabytes of storage we use in our computing centers. Our vendors are responsible for maintaining service availability of at least 99.95 percent, and they must sustain the technological currency of their hardware and software infrastructure. This partnership with the vendor community allows us to build the most efficient possible environment while reducing a myriad of operational and acquisition overhead costs that were inherent in the former process. We're also seeing a significant reduction in time to service, now averaging days instead of months to get capacity to the data center floor once a requirement has been established. Bottom line is we intend for these savings to be passed on to our customers while still maintaining high service quality.

Also, to enhance transparency, DISA is now in the process of seeking a balance sheet clean audit opinion. By the summer of 2008, our auditor—the Office of the DoD Inspector General—will judge whether DISA's financial documentation and practices are sufficient to deserve a clean audit opinion. When successful, DISA will be one of only five government organizations to have accomplished this feat. The reasons for pursuing this are compelling. We believe the practices involved with the clean audit opinion will help us to accelerate vendor payments, improve program execution, and enable DISA to build better budgets and defend them. Ultimately, it's about increasing the confidence of our customers and vendors so we can be better partners in delivering capabilities to the warfighter.

Q.

Are there any other items you'd like to share with Defense AT&L readers?

A.

We are embracing change. I sincerely believe we have some great opportunities, and responsibilities, now and in the near future, both leveraging the tremendous technology changes and learning to work even more effectively through aligned efforts within the Department. We will continue to engage with government and industry team members to do the things that raise the bar in both information sharing and network protection. The goal has been, and will continue to be, achieving the results that will best allow our warfighters and mission partners to leverage information whenever and wherever they need it to accomplish the mission. Delivering IT is a team sport.

Q.

Thank you for your time, Lt. Gen. Croom.